Al-Balqa Applied University

Prince Abdullah bin Ghazi Faculty of Information and Communication Technology

Department of Computer Science

The Curriculum for the M.Sc. Degree in

Cyber Security

Thesis Track

2021/2022

Program Objectives:

The MSc. program in cyber security enables students to master the following objectives:
PO1: Analyze and solve a cyber security problem using algorithmic techniques.
PO2: Implement and test solution(s) of a cyber security problem using appropriate tools.
PO3: Use oral and written communication and interpersonal skills to convey knowledge, ideas, and results professionally, ethically, accurately and efficiently.
PO4: Conduct scientific research and publish high quality research results and manuscripts.

Program Learning Outcomes:

At the successful completion of the MSc. program in Cyber Security, the student should be able to:

1. Demonstrate broad knowledge and understanding of current cybersecurity, cyberspace and information sciences.
2. Analyze a complex computing security problem and to apply principles of security and other relevant disciplines to identify solutions.
3. Apply security principles and practices to maintain operations in the presence of risks and threats.
4. Evaluate scientific literature, research techniques and methodologies; and formulate hypotheses, design and conduct independent and innovative research ideas applicable to their study fields.
5. Conduct experiments and analyze experimental results applied on a significant computer security problem and related to their field of study.
6. Comply with ethical issues and safety regulations related to computing and information sciences including security and data integrity, copyright, authorship, plagiarism, and use of hazardous materials.
7. Communicate effectively in a variety of professional contexts.

Knowledge Domains

No	Knowledge Domain	Course
1	Algorithms and Encryption	Applied Cryptography, Theory of Algorithms
2	Information Security	Information Security
3	Network Security	Advanced Computer Network Security
4	Security Management	Risk Assessment and Management
5	Special Topics	Scientific Research Methodology, Applications of Artificial Intelligence in Cyber Security
6	Comprehensive Exam	
9	Project & Thesis	

The curriculum consists of (33) credit hours which are distributed as follow:

Requirements	Credit Hours	Percentage
Core Courses	18	54.4%
Elective Courses	6	18.3%
Master Thesis	9	27.3%
Total	**33**	**100%**

a) Specialization Compulsory Requirements (**18** Credit Hours):

Course No.	Course	Credit Hours	Weekly Hours		Prerequisite
			Lecture	Lab.	
CYB 813	Theory of Algorithms	3	3	-	-
CYB 811	Applied Cryptography	3	3	-	-
CYB 851	Scientific Research Methodology	3	3	-	-
CYB 822	Information Security	3	3	-	-
CYB 832	Advanced Computer Network Security	3	3	-	-
CYB 841	Risk Assessment and Management	3	3	-	-
Total		**18**	**18**	**-**	

b) Specialization Elective Requirements (**6** Credit Hours):

Course No.	Course	Credi t Hours	Weekly Hours		Prerequisite
			Lecture	Lab.	
CYB 834	Information Technology Auditing and Cyber Security	3	3	-	-
CYB 821	Hacking Techniques	3	3	-	-
CYB 842	The foundations of Law and Cybercrimes	3	3	-	-
CYB 815	Building Secure Software	3	3	-	-
CYB 831	Wireless Network Security	3	3	-	-
CYB 843	Digital Evidence Investigations	3	3	-	-
CYB 854	Human and Ethical Aspects of Cyber Security	3	3	-	-

CYB 856	Special Topics in Cyber Security	3	3	-	-
CYB 852	Applications of Artificial Intelligence in Cyber Security	3	3	-	-

c) Master Thesis (**9** Credit Hours):

Course No.	**Course**	**Credit Hours**	**Weekly Hours**		**Prerequisite**
			Lecture	**Lab.**	
CYB 897	Master Thesis	9	-	-	*
Total		**9**	**-**	**-**	

*The student should successfully pass all the 18 credit hours with a GPA not less than 3.25 out of 4.

Advisory Plan

First Year					
First Semester			**Second Semester**		
No.	**Course Title**	***Credit Hours***	**No.**	**Course Title**	**Cr. Hrs.**
CYB 813	Theory of Algorithms	3	CYB 822	Information Security	3
CYB 811	Applied Cryptography	3	CYB 832	Advanced Computer Network Security	3
CYB 851	Scientific Research Methodology	3	-	Elective course	3
Total		**9**	**Total**		**9**

Second Year					
First Semester			**Second Semester**		
No.	**Course Title**	***Credit Hours***	**No.**	**Course Title**	**Cr. Hrs.**
CYB 841	Risk Assessment and Management	3	CYB 897	Master Thesis	9
-	Elective course	3			
Total		**6**	**Total**		**9**

Courses Description

Course Name	:	Theory of Algorithms	Course Number	:	CYB813
Credit Hours	:	[3] Th. : [3] Pra. : [0]	Prerequisites	:	-

The main topics covered in the course include: basics of algorithms, Asymptotic analysis of time complexity, solving recurrence relations, sorting and searching algorithms, divide and conquer(i.e. merge sort, matrix multiplication), dynamic programming (i.e. knapsack, sequence alignment shortest paths), data structures (heaps, balanced search trees (i.e. AVL trees, Red-Black trees, splay trees), hash tables, bloom filters, Disjoint sets), randomized algorithms, graph algorithms (applications of BFS and DFS, connectivity, shortest paths), max-flow algorithms; greedy algorithms (scheduling, minimum spanning trees, clustering, Huffman codes), local search and analysis of heuristics, string-processing algorithms, approximation algorithms and NP-completeness.

Course Name	:	Scientific Research Methodology	Course Number	:	CYB851
Credit Hours	:	[3] Th. : [3] Pra. : [0]	Prerequisites	:	-

Definitions and characteristics of research, research process, research tools and techniques, major considerations needed in conducting scientific research, reading research papers, analyzing research papers, presentation, types of research, topic selection, research methodology, evaluation and validation of research results, writing, publishing, presenting research work, intellectual property, plagiarism and ethics.

Course Name	:	Applied Cryptography	Course Number	:	CYB 811
Credit Hours	:	[3] Th. : [3] Pra. : [0]	Prerequisites	:	-

Public key cryptography, hash association, message authentication, RSA technology, Diffie Hellman technology, authentication powers, digital signatures, cryptographic applications, protocols and tools for analyzing these protocols. Study and design of secure communications protocols, security of cryptographic facilities, and convert this knowledge into applications.

Course Name	:	Information Security	Course Number	:	CYB822
Credit Hours	:	[3] Th. : [3] Pra. : [0]	Prerequisites	:	-

Information security basics, building information security models and techniques, including achieving physical security of information systems, security of procedures and operations, monitoring access to information and defense methods against various risks, including piracy and unauthorized access to systems. Tools to protect confidentiality of information such as encryption, secure networks and the Internet, reduce the risk of virus attacks, and attack firewalls. It also covers methods of protecting the availability and integrity of information.

Course Name	:	Advanced Computer Network Security	Course Number	:	CYB832
Credit	:	[3] Th. : [3] Pra. : [0]	Prerequisites	:	-

Hours					

This course aims to learn how computer networks operate, how they are targeted and used as a means of launching security attacks, and how we can secure and defend them. The major protocols at each layer of the protocol stack will be reviewed, known security vulnerabilities examined, countermeasures identified and explained, and security issues arising in computer networks will be considered. Through practical assignments, students will gain experience working with network protocols and learn how security attacks that involve network infrastructure can be identified.

Course Name	:	Applications of Artificial Intelligence in Cyber Security	Course Number	:	CYB852
Credit Hours	:	[3] Th. : [3] Pra. : [0]	Prerequisites	:	-

This course deals with the applications of artificial intelligence in the field of cybersecurity. Topics covered include machine learning-based intrusion detection systems, malware detection, artificial intelligence as a service, digital forensics, and incident response using machine learning.

Course Name	:	Risk Assessment and Management	Course Number	:	CYB841
Credit Hours	:	[3] Th. : [3] Pra. : [0]	Prerequisites	:	-

Information systems and risk management, layers of threats, existing risk management frameworks, models and processes, tools necessary to provide students with this theory, science, and practical knowledge to activate risk management in government and private entities, risk identification, risk assessment, prevention and mitigation of risks, risk disposal Outsourcing, advanced and supportive tools for risk management sciences.

Course Name	:	Digital Evidence Investigations	Course Number	:	CYB843
Credit Hours	:	[3] Th. : [3] Pra. : [0]	Prerequisites	:	-

This course includes the various options available to organizations in investigating problems and attacks on computer systems: a set of computer forensic frameworks and to create a framework in order to assist organizations in the systematic documentation, analysis, and resolution of cybersecurity issues; Exploitation techniques including shellcode, DLL linking and authentication eavesdropping; Use system log files, domain authentication, and registration mechanisms to obtain digital evidence. Identify the presence of the rootkit and learn to prevent attacks that focus on identifying, storing, analyzing, and displaying digital evidence related to the abuse or intrusion of an enterprise-wide system.

Course Name	:	The foundations of Law and Cybercrimes	Course Number	:	CYB842
Credit Hours	:	[3] Th. : [3] Pra. : [0]	Prerequisites	:	-

Cybercrime refers to a range of criminal activities including crimes against computer data and systems, computer-related crimes, content offenses, and copyright infringements. While early computer hackers were more interested in exploring youth, modern cybercrime is increasingly about criminal profit, and this is reflected in the involvement of transnational organized crime groups. This course covers the types of cybercrime, its perpetrators, and methods of investigation.

Course Name	:	Information Technology Auditing and Cyber Security	Course Number	:	CYB834
Credit Hours	:	[3] Th. : [3] Pra. : [0]	Prerequisites	:	-

Basic knowledge of cybersecurity auditing and process control, control framework, legal and ethical issues for information technology auditors, audit planning, information technology service provision, communication network auditing and auditing, fraud application and forensic auditing, electronic business auditing and auditing through ISO, auditing from During PCI, GLBA auditing, HIPAA audits, and SOX audits, conducting information systems audits, establishing oversight and auditing structures over the IT infrastructure, establishing systematic handling procedures

Course Name	:	Hacking Techniques	Course Number	:	CYB821
Credit Hours	:	[3] Th. : [3] Pra. : [0]	Prerequisites	:	-

The most common methods of hacking and infiltration include reconnaissance, system scanning, entry into systems through attacks on networks or applications, and denial of service attacks. This course also includes the study of methods and tools for analyzing, cleaning and monitoring movement in networks, in addition to methods of intrusion detection.

Course Name	:	Building Secure Software	Course Number	:	CYB815
Credit Hours	:	[3] Th. : [3] Pra. : [0]	Prerequisites	:	-

This course deals with the fundamentals of software security, guidelines and principles of secure coding, and advanced software security concepts. Evaluate and understand software threats. Principles for designing and implementing secure software systems. Students are expected to have practical experience in facing common security risks.

Course Name	:	Wireless network security	Course Number	:	CYB 831
Credit Hours	:	[3] Th. : [3] Pra. : [0]	Prerequisites	:	-

Mobile computing, pervasive computing, mobile devices, wireless communications, access to data everywhere, awareness, security and privacy of place and context, design methodologies and infrastructure, different attack mechanisms on a wireless network, and evaluation of the different technologies that go into designing and securing a strong wireless system.

Course Name	:	Digital Evidence Investigations	Course Number	:	CYB831
Credit Hours	:	[3] Th. : [3] Pra. : [0]	Prerequisites	:	-

Knowing the basics of solving computer crimes by learning how to identify, protect and collect evidence, and counter the retrieval of data, reports and information on digital crime to help present them to the courts by following the correct methods of investigating cybercrimes so that they can be resolved, and the perpetrators prosecuted. Read specialized studies to learn about digital crime scene investigation techniques, techniques and tools used to construct and solve computer crimes and analyze them. Also, the requirements for conducting a digital crime investigation are presented through lectures, practical exercises, scenarios and case studies.

Course Name	:	Human and Ethical Aspects of Cyber	Course Number	:	CYB854

		Security							
Credit Hours	:	[3]	Th. :	[3]	Pra. :	[0]	Prerequisites	:	-
Ethical theories, ethical attitudes and behaviors, software security, flows and the seriousness of their flow, computer misuse, software piracy, intellectual property, focus on the human element in cyberspace incidents in relation to the protection of information and technology assets, ethical aspects of codes, codes of conduct and accountability related to ethical responsibility.									

Course Name	:	Special Topics in Cyber Security					Course Number	:	CYB856
Credit Hours	:	[3]	Th. :	[3]	Pra. :	[0]	Prerequisites	:	-
Topics for this course are determined periodically by the Department Board, depending on new trends and technologies in the field of cybersecurity.									

Course Name	:	Thesis					Course Number	:	CYB897
Credit Hours	:	[3]	Th. :	[3]	Pra. :	[0]	Prerequisites	:	-
Students are required to conduct research on a well-defined topic, to develop solutions within a specified scope, to meet specific objectives and stakeholder requirements. It should be supervised by an academic supervisor to plan project milestones, adhere to ethical behavior, and protocols for design validation and verification, in addition to considering safety, security and risk factors to gain advanced theoretical and technical knowledge in the field of research.									